UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,542	09/15/2005	Peter Rostin	4414-38	1651

80167 7590 06/02/2010

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
HO, VIRGINIA T	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,542	ROSTIN ET AL.	
	Examiner	Art Unit	
	VIRGINIA HO	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the pre-appeal conference request decision mailed on March 23, 2010.

Claim Objections

2. Claim 3 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 3 recites *"wherein the seed is generated, by at least one of the seed generation client and the seed generation server, as a function of a combination of the second string* ***and one or more of****: (i) the first string, and (ii) identifying information associated with the seed generation server."* However, claim 3 is dependent upon claim 1, which recites "generating the seed as a function of **at least** the **first string** and the second string." One embodiment of claim 3 could comprise of generating a seed as a function of a combination of *a second string and identifying information associated with the seed generation server.* Another embodiment of claim 3 could comprise of generating a seed as a function of a combination of *a second string and a first string.* The last embodiment of claim 3 could comprise of generating a seed as a function of a combination of *a second string, a first string, and identifying information associated with the seed generation server.* The first two embodiments do not appear to further limit the subject matter of parent claim 1.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 36 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

5. The claim recites a "*machine-readable storage medium.*" However, the broadest reasonable interpretation of a claim drawn to a "*machine-readable storage medium*" covers forms of non-transitory tangible media and transitory propagating signals, particularly as the specification does not explicitely define what is encompassed by the term. Thus the claims may be considered to be directed to encompass non-statutory subject matter of signals per se.

A claim drawn to such a "*machine-readable storage medium*" may be amended to cover only statutory embodiments to overcome this rejection under 35 USC 101 by adding the limitation "non-transitory" to the claim and to positively state on the record a disclaimer to transitory media embodiments.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-5, 7-8, 13-14, 16, 19, 27-28, 35-40 rejected under 35 U.S.C. 102(b) as being anticipated by Chen et al. *(US Patent 5,784,463) (hereinafter Chen).*

As per claim 1, Chen teaches a method for secure generation of a seed for use in performing one or more cryptographic operations, the method comprising the steps of:

a seed generation server providing a first string to a seed generation client *(column 5, lines 7-18, server generates second portion SSK2 of the authentication key, transmits to client)*;

the seed generation client generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key, first portion is encrypted and transmitted to the authentication server)*;

the seed generation client generating the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server)*; and

the seed generation server decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key).*

As per claim 2, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed comprises a symmetric key *(column 5, lines 24-27, the authentication key is encoded or stored for use as a shared secret key during subsequent communications).*

As per claim 3, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed is generated, by at least one of the seed generation client and the seed generation server, as a function of a combination of the second string and one or

more of: (i) the first string, and (ii) identifying information associated with the seed generation server *(column 5, lines 11-13, the authentication key is generated based upon a predetermined combination of both portions; column 3, lines 14-16, the portion of the shared secret key generated by the user is sent back to the server using the server public key to encrypt the shared secret key portion).*

As per claim 4, Chen teaches the method of claim 3 as applied above. Chen additionally teaches the method wherein the identifying information associated with the seed generation server comprises a public key of the seed generation server *(column 3, lines 14-16, the portion of the shared secret key generated by the user is sent back to the server using the server public key to encrypt the shared secret key portion).*

As per claim 5, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the key utilized by the seed generation client to encrypt the second string comprises a public key of the seed generation server *(column 3, lines 14-16, the portion of the shared secret key generated by the user is sent back to the server using the server public key to encrypt the shared secret key portion).*

As per claim 7, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation client comprises or is otherwise associated with an authentication token *(column 4, lines 5-7, client nodes connected to device capable of reading a token).*

As per claim 8, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation server comprises or is otherwise associated with an authentication entity *(column 4, lines 21-30)*.

As per claim 13, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation client is associated with a first processing device and the seed generation server is associated with a second processing device *(Fig. 2, client 10, authentication server 20)*.

As per claim 14, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation client and the seed generation server communicate with one another through at least one intermediary processing device *(Fig. 1B, client 10 sends encrypted portion of name and SSK1 through communications network to authentication server 20)*.

As per claim 16, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation server initiates the seed generation process responsive to receipt of a request initiated by the seed generation client *(column 2, lines 52-53, generating a shared secret key at the time of registration; column 3, lines 41-46, anyone holding a token can register to conduct transactions via the server...)*.

As per claim 19, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the second string comprises a combination of at least two component strings, including at least a first component generated in the seed generation client by interaction with the seed generation server and a second component previously stored in the seed generation client *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key; this first portion is also combined with the user name and the encrypted first portion and user name is transmitted to the server).*

As per claim 27, Chen teaches the method of claim 1 as applied above. Chen additionally teaches the method wherein the seed generation client stores the generated seed in an authentication token *(column 5, lines 25-27, authentication key is stored in the authentication token).*

As per claim 28, Chen teaches the method of claim 1 as applied above. _ additionally teaches the method wherein the seed generation server stores the generated seed in an authentication entity *(column 2, lines 60-62, server may store the generated shared secret keys of registered clients).*

As per claim 35, Chen teaches an apparatus for secure generation of a seed for use in performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device

implementing at least one of a seed generation client and a seed generation server *(column 4, lines 21-24)*;

wherein the seed generation server provides a first string to the seed generation client *(column 5, lines 7-18, server generates second portion SSK2 of the authentication key, transmits to client)*;

the seed generation client generates a second string, encrypts the second string utilizing a key, and sends the encrypted second string to the seed generation server *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key, first portion is encrypted and transmitted to the authentication server)*;

the seed generation client generates the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server)*; and

the seed generation server decrypts the encrypted second string and independently generates the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key).*

As per claim 36, Chen teaches a machine-readable storage medium containing one or more software programs for secure generation of a seed for use in performing one or more cryptographic operations, wherein the one or more software programs when executed by a processing device implement at least one of a seed generation client and seed generation server *(Fig. 1B, client 10 features a client-server application)*;

wherein the seed generation server provides a first string to the seed generation client *(column 5, lines 7-18, server generates second portion SSK2 of the authentication key, transmits to client)*;

the seed generation client generates a second string, encrypts the second string utilizing a key, and sends the encrypted second string to the seed generation server *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key, first portion is encrypted and transmitted to the authentication server)*;

the seed generation client generates the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server)*; and

the seed generation server decrypts the encrypted second string and independently generates the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key)*.

As per claim 37, Chen teaches a method for secure generation of a seed for use in performing one or more cryptographic operations, the method being implemented in a seed generation client, the method comprising the steps of:

receiving a first string from a seed generation server *(column 5, lines 15-19)*;

generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key, first portion is encrypted and*

transmitted to the authentication server); and

generating the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server)*;

wherein the first string and the second string are configured so as to permit the seed generation server to independently generate the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key).*

As per claim 38, Chen teaches an apparatus for secure generation of a seed for use in performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device implementing a seed generation client *(column 4, lines 5-6)*;

the seed generation client being configured:

(i) to receive a first string from a seed generation server *(column 5, lines 15-19)*;

(ii) to generate a second string, to encrypt the second string utilizing a key, and to send the encrypted second string to the seed generation server *(column 4, lines 64-67, column 5, lines 1-4, client generates first portion SSK1 of an authentication key, first portion is encrypted and transmitted to the authentication server)*; and

(iii) to generate the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server)*;

wherein the first string and the second string are configured so as to permit the seed generation server to independently generate the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key).*

As per claim 39, Chen teaches a method for secure generation of a seed for use in performing one or more cryptographic operations, the method being implemented in a seed generation server, the method comprising the steps of:

providing a first string to a seed generation client *(column 5, lines 7-18, server generates second portion SSK2 of the authentication key, transmits to client)*;

receiving from the seed generation client a second string encrypted utilizing a key *(column 5, lines 4-6)*;

decrypting the encrypted second string *(column 5, lines 6-7)*; and

generating the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key)*;

wherein the first string and the second string are configured so as to permit the seed generation client to independently generate the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server).*

As per claim 40, Chen teaches an apparatus for secure generation of a seed for use in

performing one or more cryptographic operations, the apparatus comprising:

a processing device comprising a processor coupled to a memory, the processing device implementing a seed generation server *(column 4, lines 21-24)*;

the seed generation server being configured:

(i) to provide a first string to a seed generation client *(column 5, lines 7-18, server generates second portion SSK2 of the authentication key, transmits to client)*;

(ii) to receive from the seed generation client a second string encrypted utilizing a key *(column 5, lines 4-6)*;

(iii) to decrypt the encrypted second string *(column 5, lines 6-7)*; and

(iv) to generate the seed as a function of at least the first string and the second string *(column 5, lines 10-12, server combines both portions of the authentication key in a predetermined manner to form the final authentication key)*;

wherein the first string and the second string are configured so as to permit the seed generation client to independently generate the seed as a function of at least the first string and the second string *(column 5, lines 18-24, client combines the first and second portions of the authentication key using the same predetermined manner as used by the server).*

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, in view of Day *(US Patent 6,052,784)*.

As per claim 6, Chen teaches the method of claim 1 as applied above. Chen does not teach the method wherein the key utilized by the seed generation client to encrypt the second string comprises a secret key shared by the seed generation client and the seed generation server.

However, Day teaches utilizing a symmetric key to maintain confidentiality of communications *(column 5, lines 27-29)*. It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Chen to utilize a shared secret key to encrypt the second string, as Day teaches that symmetric key algorithms are "typically faster and more efficient faster and more efficient than asymmetric key cryptographic algorithms, so the confidential transmission of an authentic symmetric key advantageously improves the efficiency and speed of subsequent confidential communications" *(column 5, lines 29-34)*.

10. Claims 9, 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, in view of Yatsukawa *(US Patent 6,148,404) (previously presented)*.

As per claim 9, Chen teaches the method of claim 1 as applied above. Chen does not explicitly teach the method wherein the seed generation server sends an authentication code to the seed generation client, the authentication code proving knowledge of the generated seed and instructing the seed generation client to store the generated seed.

However, Yatsukawa teaches the method wherein the client stores the generated seed upon receipt of an authentication code by the server *(Figure 13, the client stores authentication data D_2 upon receiving a message of "grant" indicating the authentication processing result*

from the server). Notification of grant of the authentication request received from the authentication server assures that both the server's knowledge of the generated authentication data matches that of the client *(column 13, lines 23-29)*.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Chen in order send an authentication code which proves knowledge of a generated seed and instructs a client to store said seed, so as to ensure that the appropriate seed is stored by the client. Such an authentication method would make it difficult for an unauthorized entity to replace the seed which was securely generated with a false seed right before it is stored.

As per claim 29, Chen teaches the method of claim 1 as applied above. Chen does not explicitly teach the method wherein the generated seed is used to replace an existing seed known to both the seed generation client and the seed generation server. However, Yatsukawa teaches generating a seed in order to replace an existing seed known to both a client and server *(Fig. 13, after comparison of the authentication data, the client/server stores the new seed in place of the old one)*.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Chen to replace the existing seed with the newly generated seed, as Yatsukawa teaches changing the seed data and corresponding inspection data every time in order to improve resistance to replay attacks *(column 22, lines 42-45)*.

As per claim 30, Chen in view of Yatsukawa teaches the method of claim 29 as applied above. Chen in view of Yatsukawa additionally teaches the method wherein the generated seed is

used to replace an existing seed in an authentication token associated with the seed generation client and in an authentication entity associated with the seed generation server *(Yatsukawa, Fig. 13, after comparison of the authentication data, the client/server stores the new seed in place of the old one).*

As per claim 31, Chen in view of Yatsukawa teaches the method of claim 30 as applied above. Chen in view of Yatsukawa additionally teaches the method wherein the authentication token replaces the existing seed with the generated seed after the receipt of a signal from the authentication entity *(Yatsukawa, Abstract, upon receiving a grant from the server, the client stores the data as seed data in place of the first seed data).*

As per claim 32, Chen in view of Yatsukawa teaches the method of claim 31 as applied above. Chen in view of Yatsukawa additionally teaches the method wherein the signal from the authentication entity comprises an authentication code cryptographically derived from the seed *(column 11, lines 40-43, Yatsukawa teaches enciphering seed data in order to generate authentication data sent from one party to another in order to provide authentication; Fig. 13, after comparison of the authentication data, the client/server stores the new seed in place of the old one).*

As per claim 33, Chen in view of Yatsukawa teaches the method of claim 30 as applied above. Chen in view of Yatsukawa additionally teaches the method wherein the authentication entity replaces the existing seed with the generated seed after receipt of a signal from the

authentication token *(Yatsukawa, Fig. 13; column 17, lines 24-31, the server updates the authentication data D_1 received from the client X and stores as inspection data only when the collation result is coincident).*

As per claim 34, Chen in view of Yatsukawa teaches the method of claim 33 as applied above. Chen in view of Yatsukawa additionally teaches the method wherein the signal from the authentication token comprises an authentication code cryptographically derived from the seed *(column 11, lines 40-43, Yatsukawa teaches enciphering seed data in order to generate authentication data sent from one party to another in order to provide authentication; Fig. 13, after comparison of the authentication data, the client/server stores the new seed in place of the old one).*

11. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, in view of Yatsukawa, and further in view of Carro et al. *(US Pre-Grant Publication 2002/0013794) (hereinafter Carro) (previously presented).*

As per claim 10, Chen in view of Yatsukawa teaches the method of claim 9 as applied above. Chen in view of Yatsukawa does not teach the method wherein the authentication code is cryptographically derived from a secret key shared by the seed generation client and the seed generation server. More specifically, Yatsukawa teaches enciphering seed data by a secret key *(column 11, lines 40-43)* in order to generate an authentication code sent from one party to another in order to provide authentication. The authentication code taught by Yatsukawa was derived from a private key of an asymmetric key pair.

However, Carro teaches that one type of authentication code, known as a MAC, is often computed from a secret key shared only by the sender and receiver *(paragraph [0003])*. It would have been obvious for one of ordinary skill in the art at the time of the invention to further modify Chen in order to cryptographically derive the authentication code from a secret key, rather than a private key associated with the client, as doing so ensures that "only the ones sharing the secret-key are able to verify the hash" *(paragraph [0027])*.

12. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Kaliski, Jr. *(US Pre-Grant Publication 2001/0055388) (hereinafter Kaliski) (previously presented)*.

As per claim 11, Chen teaches the method of claim 1 as applied above. Chen does not explicitly teach the method wherein the seed generation server sends the generated seed to an authentication entity. However, Kaliski teaches a server which comprises or is otherwise associated with an authentication entity *(paragraph [0019], Kaliski teaches the use of verification servers, which may or may not also be the servers together with a client generate a strong secret, which may be used as a seed)*. Kaliski describes verification servers which provide authentication of the regenerated strong secret.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Chen in order to send a generated seed to an authentication entity, as doing so provides a mechanism for authentication of a generated seed created by deterministic means *(paragraph [0019], Kaliski describes how authentication could help determine if an unauthorized entity is attempting to regenerate the strong secret)*. An authenticated seed provides for a more secure

seed generation and consequently key generation. In addition, in the case where the authentication entity may not be the same as the seed generation server, it is clear that there needs to be a way for the server to send the generated seed to the authentication entity to perform appropriate authentication.

As per claim 12, Chen in view of Kaliski teaches the method of claim 11 as applied above. Chen in view of Kaliski additionally teaches the method wherein the seed generation server also sends user identifying information associated with the seed to the authentication entity *(Chen, column 6, lines 10-14)*.

13. Claim 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Fielder et al. *(US Patent No. 5963646) (hereinafter Fielder) (previously presented)*.

As per claim 15, Chen teaches the method of claim 1 as applied above. Chen does not teach the method wherein the seed generation server initiates the seed generation process responsive to receipt of a command. However, Fielder teaches generating a seed, wherein an activation code initiates the generation of this process *(column 3, lines 22-33; column 7, lines 38-40)*. It would have been obvious for one of ordinary skill in the art at the time of the invention to modify the Chen in order to initiate generation of a seed based upon receipt of a command, as this would allow the party that submits the command to direct the generation of the seed as needed, giving an increased level of control which allows the seed generation process to be "automated" and efficient.

14. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, in view of Huima *(Pre-Grant Publication 2002/0164026)*.

As per claims 17 and 18, Chen teaches the method of claim 16 as applied above. Chen does not explicitly teach the method wherein the seed generation client in response to initiation of the seed generation process by the seed generation server provides the seed generation server with information indicating one or more processing algorithms suitable for use in the seed generation process, and wherein the seed generation server responsive to the information indicating one or more processing algorithms provides to the seed generation client additional information specifying one or more characteristics of the seed generation process.

However, Huima teaches two parties exchanging the values of parameters *(paragraph [0019])* such as security parameters "used to inform the other party about available ciphers, hash functions etc." *(paragraph [0052])*. It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Chen to indicate one or more processing algorithms used in the seed generation process, as Huima teaches that this allows for the calculation of a shared secret *(paragraph [0019])*, and doing so ensures that both the client and server know which algorithm to use to generate the key, as Chen teaches that the client and server are able to generate the key based on any predetermined manner *(column 5, lines 11-24)*.

15. Claims 20-21 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Fielder, and further in view of Burnett et al. *(2001) (hereinafter Burnett) (previously presented)*.

As per claim 20, Chen teaches the method of claim 1 as applied above. Chen does not teach the method wherein the seed is generated by repeatedly applying a cryptographic algorithm to successive portions of an additional string generated utilizing the first string, the second string and the key.

However, Fielder teaches the method wherein the seed is generated by applying a cryptographic algorithm to an additional string generated utilizing the first string, the second string, and the key *(column 3, lines 50-52, the first string, a constant value, may combined with a second string, the E-Key seed, through a sequence of cryptographic steps to provide an input (seed) to a secure hash function; column 3, lines 53-55, the E-Key seed and constant value may be encrypted)*.

It would have been obvious for one or ordinary skill in the art at the time of the invention to modify Chen in order apply a block cipher with a feedback mode by repeatedly applying the cryptographic algorithm to successive portions of the additional string, as Burnett teaches that a block cipher comprises one type of symmetric key algorithm and utilizing a feedback mode solves the problem of copies of ciphertext resulting from applying a block cipher, which an attacker might identify as a repeated pattern *(pp. 40)*. By repeatedly applying the algorithm to portions of the additional string, the seed appears more random, and therefore becomes more resistant to attacks.

As per claim 21, Chen in view of Fielder and Burnett teaches the method of claim 20 as applied above. Chen in view of Fielder and Burnett additionally teaches the method wherein the additional string generated utilizing the first string, the second string and the key comprises a

concatenation of the first string, the second string and the key *(Fielder, column 3, lines 49-52, a constant value, the first string, may be combined with the E-Key seed, the second string, through a sequence of logic, algebraic, and/or cryptographic steps).* It would have been obvious to one of ordinary skill in the art at the time of the invention to concatenate the first string, the second string, and the key prior to applying a cryptographic algorithm to the generated string in order to produce a seed, as concatenation is one of the simplest methods of combining two bit sequences.

As per claim 25, Chen in view of Fielder and Burnett teaches the method of claim 20 as applied above. Chen in view of Fielder and Burnett additionally teaches the method wherein the cryptographic algorithm comprises an encryption operation *(Fielder, column 2, lines 23-25, encryption algorithms are required to generate an encryption key, which may be used as a seed, as stated earlier).*

16. Claims 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Fielder, and further in view of Burnett, and further in view of Scheidt et al. *(US Pre-Grant Publication 2002/0062451) (hereinafter Scheidt) (previously presented).*

As per claim 22, Chen in view of Fielder and Burnett teaches the method of claim 20 as applied above. Chen in view of Fielder and Burnett does not teach the method wherein the additional string comprises n portions C[1], C[2],... C[n], and the seed is generated by computing:

I[1] -- Algorithm (C[1], C[2])

I[2] -- Algorithm (I[1], C[3])

...

I[n- 1] = Algorithm (I[n-2], C[n])

seed = I[n-1],

where Algorithm (A, B) denotes application of the cryptographic algorithm to portion B of the string utilizing an algorithm parameter denoted by A.

However, Scheidt teaches the method wherein a working key is constructed from several pieces of information via a combiner function *(paragraph [0056])*. This working key is used to initialize a symmetric key cryptographic algorithm. Scheidt teaches the working key generated by applying a combiner function such as Triple DES in CBC Mode *(Figure 5)*. CBC Mode is a type of feedback mode. The algorithm claimed in 22 demonstrates a type of block cipher utilizing a type of feedback mode. It would have been obvious for one of ordinary skill in the art at the time of the invention that rather than using an IV as an algorithm parameter, the algorithm could be applied to the second portion of the string, with the first string functioning as the IV instead. Utilizing the first string as the first parameter eliminates the need to generate a separate value to be used as the IV.

Additionally, it would have been obvious for one of ordinary skill in the art at the time of the invention to further modify Chen, in order to generate a shared secret key using such an algorithm, as utilizing "splits," or components, in the manner taught by Scheidt to generate a working key, as Scheidt teaches that the combiner function "is particularly advantageous for use with applications that have relatively limited resources" *(paragraph [0093])*.

17. Claims 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, in view of Fielder, further in view of Burnett, and further in view of Huima.

As per claims 23 and 24, Chen in view of Fielder and Burnett teaches the method of claim 20 as applied above. Chen in view of Fielder and Burnett does not teach the method wherein the cryptographic algorithm comprises a one-way cryptographic operation, and wherein the one-way cryptographic operation comprises a hash function. However, Huima teaches "different keys are derived from key material using different parametrized hash functions" wherein the shared secret and two nonces provide the key material *(paragraph [0050])*. It would have been obvious for one of ordinary skill in the art at the time of the invention to further modify Chen to apply a one-way hash function to the additional string generated utilizing the first string, the second string, and the key, as Huima teaches that hash functions are advantageous in providing a secure method of communication *(paragraphs [0012-0014])*.

18. Claims 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen in view of Fielder, and further in view of Burnett, and further in view of Trimberger *(US Patent 7,366,306)*.

As per claim 26, Chen in view of Fielder and Burnett teaches the method of claim 25 as applied above. Chen in view of Fielder, Burnett does not teach the method wherein the encryption operation comprises the AES algorithm.

However, it would have been obvious for one of ordinary skill in the art at the time of the invention to further modify Chen to utilize AES, as Trimberger teaches that AES is a more secure encryption algorithm *(column 1, lines 36-44)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VIRGINIA HO whose telephone number is 571-270-7309. The examiner can normally be reached on Mon to Thu; 8:30 AM - 5:00 PM (Eastern).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VIRGINIA HO/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432